

REMARKS

Claims 1-35, 69-79, 88, and 89 are pending. Claims 1, 69, 88, and 89 are in independent form.

Claim 1 was rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,738,814 to Cox et al. (hereinafter "Cox").

Claim 1 relates to a method for automatically identifying common content to use in identifying an intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the network attack, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, and analyzing a plurality of said reduced data items to detect common elements, said analyzing reviewing for common content indicative of a network attack. The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item; and

As best understood, the rejection of claim 1 contends that Cox's data packets are such reduced data items. The reason for this confusion stems from the Response to Remarks in the Office action mailed May 23, 2008. In particular, the Office action contends:

"[i]n response to Applicant argument that the Cox reference does not teach or suggest data reduction or packetization, Examiner respectfully disagrees and in addition to the previous citation and obvious reasoning as explained in previous office action, the Cox et al. is silent in disclosing the carrying out a data reduction on said portion, however it would have been obvious to one of ordinary skill in the art to modify the disclosed invention to reduce said data portions. This would be obvious to one of ordinary skill in the art because one of ordinary skill would know that the "data packets (col. 1 lines 60-67 of Cox)" - which by definition are **reductions of the original data** (hence the name "packet") - are better handled and analyzed in smaller portions. Therefore, motivation and benefit for this modification would be to allow for the received packet to be properly analyzed." See Office action mailed May 23, 2008, page 2, para. 1.2 (emphasis in original).

However, claim 1 stands rejected under 35 U.S.C. § 102(e) as anticipated by Cox in both the Office action mailed October 4, 2007 and the Office action mailed May 23, 2008. See, e.g., Office action mailed May 23, 2008, page 4 (describing that the Examiner "understands the data packet of Cox et al. to read upon and be the result of data reduction as claimed by the Applicant.").

If the above excerpt from the Response to Remarks acknowledges that Cox's data packet are not reduced data items as recited in claim 1 but instead seeks to establish a new ground of rejection- namely, an obviousness rejection under 35 U.S.C. § 103(a)- Applicant respectfully requests that the

rejections under 35 U.S.C. § 102(e) be withdrawn and a new Office action be issued to fully set forth the new obviousness rejection.

As for the contention on which the anticipation rejection is based, namely, "the data packet of Cox et al. [is understood] to read upon and be the result of data reduction as claimed," Applicant respectfully disagrees. In claim 1, the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

Cox's packetization neither describes nor suggests such a data reduction. Submitted herewith as Appendix A is a description of "What is a Packet?" printed from the "howstuffworks.com" webpage on July 14, 2008. Available at <http://computer.howstuffworks.com/question525.htm>.

As described therein by way of example, an e-mail message can be broken into packets.

"Let's say that you send an e-mail to a friend. The e-mail is about 3,500 bits (3.5 kilobits) in size. The network you send it over uses fixed-length packets of 1,024 bits (1 kilobit). The header of each packet is 96 bits long and the trailer is 32 bits long, leaving 896 bits for the payload. To break the 3,500 bits of message into packets, you will need four packets (divide 3,500 by 896). Three packets will contain 896 bits of payload and the fourth will have 812 bits. Here is what one of the four packets would contain:

Packet - E-mail Example

Header	Sender's IP address Receiver's IP address Protocol Packet number	96 bits
Payload	Data	896 bits
Trailer	Data to show end of packet Error correction	32 bits

©2000 How Stuff Works

Applicant respectfully submits that, while such data packets are indeed smaller than the original e-mail message, such packets are not reduced data items as recited in claim 1. In this regard, there does not appear to be any mechanism whereby messages that differ are reduced to the same reduced data item. For example, even if the exact same message were sent from the exact same sender to the exact same receiver using the exact same protocol, the packet numbers and hence the packets would differ. Moreover, such variability in packet numbers ensures that the packets do not have a constant predetermined relation with such e-mails.

Since Cox does not provide any additional details regarding his packets, there is no reason to believe that Cox's packets are reduced data items, as recited in claim 1. Accordingly, claim 1 is not anticipated by Cox. applicant respectfully requests that the rejections of claim 1 and the claims dependent therefrom be withdrawn.

Claim 69 was rejected under 35 U.S.C. § 102(e) as anticipated by Cox.

Claim 69 relates to a method for automatically identifying common content to use in identifying an intrusive network attack. The method includes monitoring network content on a network and obtaining at least portions of the data on said network, data reducing said portions of the data using a data reduction function which reduces said portions of the data to reduced data portions in a repeatable manner such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced data portion, analyzing said reduced data portions to find network content which repeats a specified number of times and to establish said network content which repeats said specified number of times as frequent content, identifying address information of said frequent content, and identifying the frequent content as associated with the network attack based on said identifying and determining.

The address information includes at least one of source information or destination information that characterizes the respective of sources and/or destinations of said frequent content and determining if a number of sources and/or destinations of said frequent content is increasing.

Cox neither describes nor suggests data reducing portions of data using a data reduction function which reduces the portions of the data to reduced data portions in a repeatable manner such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced data portion, as recited in claim 69.

In this regard, as discussed above, there is no reason to believe that Cox reduces e-mails that have the same content to the same packets and at least some e-mails that differ are reduced to the same packets. Accordingly, claim 69 is not anticipated by Cox. Applicant respectfully requests that the rejections of claim 69 and the claims dependent therefrom be withdrawn.

Claim 88 was rejected under 35 U.S.C. § 102(e) as anticipated by Cox.

Claim 88 relates to a method for automatically identifying common content to use in identifying an intrusive network attack. The method includes obtaining a collection of data

items to be analyzed to identify the network attack, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, analyzing a plurality of said reduced data items to determine frequently occurring sections of message information indicative of a network attack, and carrying out an additional test on said frequently occurring sections of message information.

The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

Cox neither describes nor suggests reducing data items to reduce a data collection to a reduced data collection of reduced data items, wherein the reduced data items have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item, as recited in claim 88.

In this regard, as discussed above, there is no reason to believe that Cox reduces at least some e-mails that differ to the same packets e-mails but with a constant predetermined relation with the e-mails.

Accordingly, claim 88 is not anticipated by Cox. Applicant respectfully requests that the rejections of claim 88 and the claims dependent therefrom be withdrawn.

Claim 89 was rejected under 35 U.S.C. § 102(e) as anticipated by Cox.

Claim 89 relates to a method for automatically identifying common content to use in identifying an intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items comprise a first subset of a network packet including payload and header, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, analyzing a plurality of said reduced data items to detect common elements, and obtaining a second subset of the same network packet for subsequent analysis.

The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

In this regard, as discussed above, there is no reason to believe that Cox reduces at least some e-mails that differ to the same packets e-mails but with a constant predetermined relation with the e-mails.

Accordingly, claim 89 is not anticipated by Cox. Applicant respectfully requests that the rejections of claim 89 and the claims dependent therefrom be withdrawn.


It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. For example, applicant does not respond to the comments responding to Applicant's remarks regarding the obviousness rejections of former claims 12, 19 since claims 88, 89 stand rejected under 35 U.S.C. § 102(e) over Cox.

In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant asks that all claims be allowed. No fees are believed due at this time. Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: July 15, 2008



John F. Conroy
Reg. No. 45,485

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

JFC/jhg
10848299.doc

A service of Discovery Communications Inc.

Video Center Maps Consumer Guide: Auto
Reviews / Product Reviews

Make HowStuffWorks your homepage | Get Newsletter | RSS

howstuffworks

Search HowStuffWorks and the web

search powered by Google

Home Adventure Animals Auto Communication Computer Electronics Entertainment Food Geography

Health History Home & Garden Money People Science

Computer Hardware ▼ Computer Peripherals ▼ Computer Security ▼ Computer Software ▼ Internet ▼

Home > Computer > Computer Hardware > Networking

What is a packet?

Print Email Own Print

It turns out that everything you do on the Internet involves **packets**. For example, every Web page that you receive comes as a series of packets, and every e-mail you send leaves as a series of packets. Networks that ship data around in small packets are called **packet switched networks**.

On the Internet, the network breaks an e-mail message into parts of a certain size in **bytes**. These are the packets. Each packet carries the information that will help it get to its destination -- the sender's IP address, the intended receiver's IP address, something that tells the network how many packets this e-mail message has been broken into and the number of this particular packet. The packets carry the data in the protocols that the Internet uses: Transmission Control Protocol/Internet Protocol (TCP/IP). Each packet contains part of the body of your message. A typical packet contains perhaps 1,000 or 1,500 bytes.

Each packet is then sent off to its destination by the best available route -- a route that might be taken by all the other packets in the message or by none of the other packets in the message. This makes the network more efficient. First, the network can balance the load across various pieces of equipment on a millisecond-by-millisecond basis. Second, if there is a problem with one piece of equipment in the network while a message is being transferred, packets can be routed around the problem, ensuring the delivery of the entire message.

Depending on the type of network, packets may be referred to by another name:

- frame
- block
- cell

Computer Videos



Don't be embarrassed,
we've answered it all.
Politics explained. Click here >



Ads by Google

Full 20G Pattern Matching

1M Flows, 100K New Flows Per
Second Upto 2M Characters for
all Patterns
www.napatech.com

Cisco NetFlow Challenge

Immediate results with
NetFlow. Take our analysis
challenge.
Plixer.com/NetFlowChallenge

Deep Packet Inspection

10Gbps DPI processing
performance in a compact
network appliance
www.Bivio.net/DPISecurity

- segment

Most packets are split into three parts:

- **header** - The header contains instructions about the data carried by the packet. These instructions may include:
 - Length of packet (some networks have fixed-length packets, while others rely on the header to contain this information)
 - Synchronization (a few bits that help the packet match up to the network)
 - Packet number (which packet this is in a sequence of packets)
 - Protocol (on networks that carry multiple types of information, the protocol defines what type of packet is being transmitted: e-mail, Web page, streaming video)
 - Destination address (where the packet is going)
 - Originating address (where the packet came from)
- **payload** - Also called the **body** or **data** of a packet. This is the actual data that the packet is delivering to the destination. If a packet is fixed-length, then the payload may be **padded** with blank information to make it the right size.
- **trailer** - The trailer, sometimes called the **footer**, typically contains a couple of bits that tell the receiving device that it has reached the end of the packet. It may also have some type of error checking. The most common error checking used in packets is **Cyclic Redundancy Check (CRC)**. CRC is pretty neat. Here is how it works in certain computer networks: It takes the sum of all the 1s in the payload and adds them together. The result is stored as a hexadecimal value in the trailer. The receiving device adds up the 1s in the payload and compares the result to the value stored in the trailer. If the values match, the packet is good. But if the values do not match, the receiving device sends a request to the originating device to resend the packet.

As an example, let's look at how an e-mail message might get broken into packets. Let's say that you send an e-mail to a friend. The e-mail is about 3,500 bits (3.5 kilobits) in size. The network you send it over uses fixed-length packets of 1,024 bits (1 kilobit). The header of each packet is 96 bits long and the trailer is 32 bits long, leaving 896 bits for the payload. To



break the 3,500 bits of message into packets, you will need four packets (divide 3,500 by 896). Three packets will contain 896 bits of payload and the fourth will have 812 bits. Here is what one of the four packets would contain:

Packet - E-mail Example

Header	Sender's IP address Receiver's IP address Protocol Packet number	96 bits
Payload	Data	896 bits
Trailer	Data to show end of packet Error correction	32 bits

©2000 New Staff Media

Each packet's header will contain the proper protocols, the originating address (the IP address of your computer), the destination address (the IP address of the computer where you are sending the e-mail) and the packet number (1, 2, 3 or 4 since there are 4 packets). Routers in the network will look at the destination address in the header and compare it to their lookup table to find out where to send the packet. Once the packet arrives at its destination, your friend's computer will strip the header and trailer off each packet and reassemble the e-mail based on the numbered sequence of the packets.

Here are some interesting links:

- [How Ethernet Works](#)
- [How Cell Phones Work](#)
- [How the Internet and Web Servers Work](#)
- [How Home Networks Work](#)
- [How Routers Work](#)
- [whatis.com's definition of a packet](#)

Ads by Google

IP Phone System

PC Mags Top Rated PBX. Outlook Integration & Unlimited Extensions.
Fonality.com/IP

Network Admin Degree

Take hands on courses & earn your degree at University of Phoenix.
Phoenix.edu

Free Nortel BCM Quote

Lowest price guaranteed! Visit or Call 1-800-564-8045
StarTechTel.com

Related Ad Categories

Network Computer
Network Diagrams
Networking Books

DSL Router
Wireless LANs

Search HowStuffWorks and the web

search

enhanced by Google

[Home](#) | [Adventure](#) | [Animals](#) | [Auto](#) | [Communication](#) | [Computer](#) | [Electronics](#) | [Entertainment](#) | [Food](#) | [Geography](#) | [Health](#) | [History](#) | [Home & Garden](#) | [Money](#) | [People](#) | [Science](#)



SoundWorks' i765 | iPod/DVD Entertainment System
New Only: \$299.99!
 Dock & Play iPod, DVD/DVD Player, AM/FM Radio & more!



www.cambridgesoundworks.com

[HSW Brazil](#) | [Company Info](#) | [Advertise With Us](#) | [Newsletter](#) | [Careers](#) | [Privacy](#) | [Contact Us](#) | [Help](#) | [Terms & Conditions](#) | [RSS](#)

© 1998-2008 HowStuffWorks, Inc.

[Discovery Communications, LLC](#) | [Discovery Channel](#) | [TLC](#) | [Animal Planet](#) | [Discovery Health](#) | [Science Channel](#) | [Planet Green](#) | [Discovery Kids](#)
[Potfinder](#) | [TreeHugger](#) | [Military Channel](#) | [Investigation Discovery](#) | [HD Theater](#) | [FitTV](#) | [Turbo](#)